October 26, 2010

Via ECFS
Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: Notice of Ex Parte Presentation: Public Notice, FCC Seeks Public Comment on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap (PS Docket No. 10-146 and GN Docket No. 09-51); Cyber Security Certification Program (PS Docket 10-93); Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment Or Severe Overload (PS Docket No. 10-92)

Dear Ms. Dortch:

On October 25, 2010, Adam Golodner, Director, Government Affairs, Ken Watson, Senior Manager, Government Affairs and the undersigned met with the following Public Safety and Homeland Security Bureau officials to discuss various issues in the above-captioned dockets: Jennifer Manner, Deputy Chief, Jeffrey Goldthorp, Associate Chief, Lisa Fowlkes, Deputy Chief, Jane Kelly and Vern Mosley. During the course of the meeting, Cisco staff were asked a number of questions about various cybersecurity issues and the potential role of the FCC in addressing those issues.

In sum, Cisco staff offered the following opinions: (1) industry and government have various preferred approaches in improving the security of border gateway protocol technology, and at this time, industry is addressing this area through "best practices" approaches; (2) regarding DNSSEC, the Internet Corporation for Assigned Names and Numbers (ICANN) has made progress (pursuant to agreement) with the signing of the root, and ICANN and others continue to do good work on Domain Name System security; (3) network resiliency is an important issue, and continued work here best effectuated through a public-private partnership approach in lieu of a government mandate; (4) improvements in user security by Internet Services Providers would also benefit from a public-private partnership approach, where service providers and government partners can exchange ideas, challenges and actions to improve user security; and (5) while industry and government agree that there is an issue with respect to identifying servers that are responsible for spam or other malicious content, the issue is global, often involves law enforcement, and, again can benefit from trusted discussion about approaches to improve security.

In addition, Cisco provided an online pointer to FCC staff containing the baseline risk assessment report for the IT sector conducted by the IT Sector Coordinating Council and the IT

Government Coordinating Council, chaired by the Department of Homeland Security in 2009. http://www.us-cert.gov/reading_room/IT_Sector_Risk_Assessment_Report.pdf

More broadly, Cisco noted that important strides have been made in cyber security, attention to the issue, and protecting networks from cyber incidents, and that much of the work had been built on the foundation of public-private partnerships, extensive trust relationships between the market and government participants, and the aligned incentives of the public sector and the IT and IT dependant industries to continue to drive trust across networks. In contrast, where governments elsewhere in the world deviate from the use of international standards, best-practices, and public-private partnerships, those divergent government directed actions tend to pull apart interoperability and security, lead toward a balkanization of the Internet, and retard the growth of the global benefits from a robust interconnected network. Cisco has consistently pointed to the US process, with its heavy reliance on public private partnerships, as a model for what the rest of the world should use in addressing cyber security issues.

Sincerely,

Mary L. Brown

Mary L. Brown
Director, Government Affairs

CC:
Jennifer Manner
Lisa Fowlkes
Jeff Goldthorp
Jane Kelly
Vern Mosely